NIST Special Publication 800-59
DRAFT [Version 0.3]

Guideline for Identifying an Information System as a National Security System

U.S. DEPARTMENT OF COMMERCE

Technology Administration
National Institute of Standards
and Technology

William C. Barker

C O M P U T E R S E C U R I T Y

Security Technology Group
Computer Security Division
National Institute of Standards
and Technology
Gaithersburg, MD 20899-8930

June 3, 2003

U.S. Department of Commerce
Donald L. Evans, Secretary

Technology Administration
Phillip J. Bond, Under Secretary of Commerce for Technology

National Institute of Standards and Technology
Arden L. Bement, Jr., Director

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure for information technology. ITL develops tests, test methods, reference data, proof of concept implementations and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in federal computer systems. This Special Publication 800 series reports on ITL's research, guidance, and outreach efforts in computer security, and its collaborative activities with industry, government, and academic organizations.

National Institute of Standards and Technology, Special Publication 800-59
Natl. Inst. Stand. Technol. Spec. Publ. 800-59, 20 pages (*June 2003*)
CODEN: NSP*???*

GUIDELINE FOR IDENTIFICATION OF INFORMATION SYSTEMS AS NATIONAL SECURITY SYSTEMS

Table of Contents

Table of Contents iii
1.0 Introduction 1
2.0 Glossary of Terms 3
3.0 Basis for Identification of National Security Systems 7
4.1 Determination and Reporting Responsibilities 9
4.2 National Security System Identification Checklist 9
4.2.1 Intelligence Activities 10
4.2.2 Cryptologic Activities 10
4.2.3 Command and Control of Military Forces 10
4.2.4 Weapons and Weapons Systems 10
4.2.5 Systems Critical to the Direct Fulfillment of Military or Intelligence Missions 11
4.2.6 Classified Systems 11
4.3 Dispute Resolution 11
Appendix A: National Security System Identification Checklist 13
Appendix B: References 15

This page intentionally left blank.

1.0 Introduction

This document provides guidelines developed in conjunction with the Department of Defense, including the National Security Agency, for identifying an information system as a national security system consistent with applicable requirements for national security systems as specified in Title III to Public Law 107-347, the Federal Information Systems Management Act of 2002 (FISMA).

The FISMA provides a framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets and provides for the maintenance of minimum controls required to protect Federal information and information systems. Federal agencies are responsible for providing information security protection of information collected or maintained by or on behalf of the agency and information systems used or operated by or on behalf of the agency. The head of each Federal agency is also responsible for (1) assessing the risk and magnitude of the harm that could result form unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems that support operations or assets under their control; (2) determining the levels of information security appropriate to protect such information and information systems; (3) implementing policies and procedures to cost-effectively reduce risks to an acceptable level; and (4) periodically testing and evaluating information security controls and techniques to ensure that they are effectively implemented.

Except for the case of national security systems, the Secretary of Commerce, on the basis of standards and guidelines developed by NIST is responsible for prescribing standards and guidelines pertaining to Federal information systems. The National Security Agency and other intelligence community agencies provide security standards and guidance for the national security systems. The FISMA defines the term *national security system* and requires NIST to provides guidelines for identifying an information system as a national security system. This guideline provides the basis and procedure for identification of national security systems.

This page intentionally left blank.

2.0 Glossary of Terms

Definitions of terms provided in this glossary have been extracted from public laws, Executive Branch publications and orders, and American National Standards Institute publications. The numbers in brackets [*n*] associated with each definition refer to reference numbers in Appendix B.

Agency - The term 'agency' means any executive department, military department, government corporation, government controlled corporation, or other establishment in the executive branch of the government (including the Executive Office of the President), or any independent regulatory agency, but does not include -

(a) the General Accounting Office;
(b) Federal Election Commission;
(c) the governments of the District of Columbia and of the territories and possessions of the United States, and their various subdivisions; or
(d) Government-owned contractor-operated facilities, including laboratories engaged in national defense research and production activities. [3]

Availability - The term 'availability' means ensuring timely and reliable access to and use of information. [4]

Classified Information –
Classified information or classified national security information means information that has been determined pursuant to E.O. 13292 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form. [7]

Command and Control –
'Command and Control' is the exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. [10]

Confidentiality - The term 'confidentiality' means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information. [4]

Counterintelligence –
The term 'counterintelligence' means information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. [6]

Cryptologic - The term 'cryptologic' means of or pertaining to cryptology. [10]

Cryptology - 'Cryptology' is the science that deals with hidden, disguised, or encrypted communications. It includes communications security and communications intelligence. [10]

Director - The term 'Director' means the Director of the Office of Management and Budget. [3]

Independent Regulatory Agency –
The term 'independent regulatory agency' means the Board of Governors of the Federal Reserve System, the Commodity Futures Trading Commission, the Consumer Product Safety Commission, the Federal Communications Commission, the Federal Deposit Insurance Corporation, the Federal Energy Regulatory Commission, the Federal Housing Finance Board, the Federal Maritime Commission, the Federal Trade Commission, the Interstate Commerce Commission, the Mine Enforcement Safety and Health Review Commission, the National Labor Relations Board, the Nuclear Regulatory Commission, the Occupational Safety and Health Review Commission, the Postal Rate Commission, the Securities and Exchange Commission, and any other similar agency designated by statute as a Federal independent regulatory agency or commission. [3]

Information Resource –
The term 'information resources' means information and related resources, such as personnel, equipment, funds, and information technology. [3]

Information Security -
The term 'information security' means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability. [3]

Information System - The term 'information system' means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. [3]

Information Technology –

The term 'information technology', with respect to an executive agency means any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which (i) requires the use of such equipment, or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term "information technology" includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. The term "information technology" does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract. [2]

Integrity - The term 'integrity' means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [4]

Intelligence - The term 'intelligence' means (1) the product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas; or (2) information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding. [10] The term 'intelligence' includes foreign intelligence and counterintelligence. [6]

Intelligence Activities –

The term 'intelligence activities' includes all activities that agencies within the Intelligence Community are authorized to conduct pursuant to Executive Order 12333, United States Intelligence Activities. [15]

Intelligence Community –

The term 'intelligence community' refers to the following agencies or organizations:
(1) The Central Intelligence Agency (CIA);
(2) The National Security Agency (NSA);
(3) The Defense Intelligence Agency (DIA);

(4) The offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs;
(5) The Bureau of Intelligence and Research of the Department of State;
(6) The intelligence elements of the Army, Navy, Air Force, and Marine Corps, the Federal Bureau of Investigation (FBI), the Department of the Treasury, and the Department of Energy; and
(7) The staff elements of the Director of Central Intelligence. [15]

Public Information - The term 'public information' means any information, regardless of form or format, that an agency discloses, disseminates, or makes available to the public. [3]

Telecommunications –

The term 'telecommunications' means the transmission, between or among points specified by the user, of information of the user's choosing, without change in the form or content of the information as sent and received. [5]

Weapons System - A 'weapons system' is a combination of one or more weapons with all related equipment, materials, services, personnel, and means of delivery and deployment (if applicable) required for self-sufficiency. [10]

3.0 Basis for Identification of National Security Systems

The basis for the identification of 'national security systems' is defined in 44 United States Code (USC), Chapter 35, Subchapter I, Section 3502 [3]; Public Law 104-106, Division E, Section 5142 [9]; and Public Law 107-347, Subchapter III, Section 3542(b)(2) [11]. In all three documents, the term 'national security system' means any *information system* (including any *telecommunications* system) used or operated by an *agency* or by a contractor of an *agency*, or other organization on behalf of an *agency* --

(1) the function, operation, or use of which—

(a) involves *intelligence activities*;
(b) involves *cryptologic* activities related to national security;
(c) involves *command and control* of military forces;
(d) involves equipment that is an integral part of a weapon or *weapons system*; or
(e) is critical to the direct fulfillment of military or *intelligence* missions; or

(2) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified[1] in the interest of national defense or foreign policy.

Systems not meeting any of these criteria are not national security systems. Additionally, systems that do not involve 1) *intelligence activities*, 2) *cryptologic* activities related to national security, 3) *command and control* of military forces, 4) equipment that is an integral part of a weapon or *weapons system* or 5) information classified by an act of Congress or under an Executive order are not designated as national security systems if they are used exclusively for routine business or administrative applications even if they are critical to the direct fulfillment of military or *intelligence* missions. Routine business or administrative applications are defined by the laws as including payroll, finance, logistics, and personnel management applications.

[1] * See Glossary definition for *classified information*. See [7] for Executive Orders 13292 under the authority of which information may be classified.

This page intentionally left blank.

4.0 Method for Identifying National Security Systems

4.1 Determination and Reporting Responsibilities

The head of each *agency* is responsible for designating an *agency* security official to determine which, if any, *agency* systems are national security systems.

For each *information technology* system under its control, each *agency* will need to answer each of the questions stated in the National Security System Identification Checklist provided as Appendix A to this guideline. If the answer to any of the questions is affirmative, the system is designated a national security system.

If the manager of a military or intelligence mission determines that a system is critical to that mission, and the system has not previously been identified as a *national security system*, the manager responsible for that mission must so identify the system to the responsible entity designated by the head of the *agency* that owns and/or operates the system (see Section 4.2.5). The *agency* is responsible for notifying the Committee for National Security Systems (CNSS) whenever one of its systems is designated as being critical to the direct fulfillment of a military or intelligence mission. Such notification must be submitted to the CNSS Secretariat (I42), National Security Agency, 9800 Savage Road, STE 6717, Ft. George G. Meade, Maryland, 20755-6716.[2]

When the manager of a military or intelligence mission determines that a system is no longer critical to that mission, or when the mission is terminated, the manager responsible for that mission must so notify the responsible entity designated by the head of the *agency* that owns and/or operates the system, and the system ceases to be designated a *national security system*. Such change from national security status must be immediately reported to the CNSS.

Note that use of the specific form provided in Appendix A is not mandatory. Agencies may develop and use an alternate methodology. However, a record of answers to each of the questions listed on the checklist will need to be established and maintained by each Federal government *agency*.

Under the Federal Information Security Management Act of 2002 [11] each *agency* should make an annual report to the Director, Office of Management and Budget, that identifies each national security system under the authority and control of the *agency* and the basis for identifying the system as a national security system.

4.2 National Security System Identification Checklist

The National Security System Identification Checklist provided in Appendix A includes six questions. An affirmative answer to one or more of the six questions will result in the system being designated as a national security system.

[2] Electronic mail address is ntissc@radium.ncsc.mil.

4.2.1 Intelligence Activities

For purposes of this guideline, the term *intelligence activity* means all activities that agencies within the Intelligence community are authorized to conduct pursuant to E.O 12333. As authorized by statute (e.g., 10 USC 124, Chapter 18 [1], Public Law 107-296 [11]), *intelligence activities* may also include counter drug or counter terrorism *intelligence* other than that concerning foreign countries or areas concerning foreign countries or areas if the *intelligence* information was collected or developed by an organization or organizations subordinate to the Director of Central Intelligence or National Foreign Intelligence Programs subordinate to the Secretary of Defense. Box 1 should be marked yes if and only if the function, operation, or use of the system involves *intelligence activities* as defined herein.

4.2.2 Cryptologic Activities

For purposes of completing the National Security System Identification Checklist, *cryptologic* activities include signals intelligence activities, covered under intelligence activities, and the solutions, products, and services to ensure the availability, integrity, authentication, confidentiality, and non-repudiation of national security telecommunications and information systems. Box 2 should be marked yes if and only if the function, operation, or use of the system involves *cryptologic* activities as defined herein.

4.2.3 Command and Control of Military Forces

For purposes of this guideline, *command and control* is the exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. *Command and control* functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. Box 3 of the National Security System Identification Checklist should be marked yes if and only if the function, operation, or use of the system involve *command and control* of military forces.

4.2.4 Weapons and Weapons Systems

For purposes of this guideline, weapons are defined as being limited to weapons owned by and/or under the control of military forces of the United States and any weapons of mass destruction.[3] A *weapons system* is a combination of one or more weapons with all related equipment, materials, services, personnel, and means of delivery and deployment (if applicable) required for self-sufficiency. Box 4 of the National Security System Identification Checklist should be marked yes if and only if the system involves equipment that is an integral part of a weapon or *weapons system* as defined herein.

[3] The term *weapon*, as used herein, encompasses kinetic weapons, other nuclear/biological/chemical (NBC) weapons and computer network attack (CNA) weapons.

4.2.5 Systems Critical to the Direct Fulfillment of Military or Intelligence Missions

Systems that are critical to the direct fulfillment of military or *intelligence* missions are designated as national security systems unless they are to be used exclusively for routine administrative and business applications. Examples of routine administrative and business systems include those having payroll, finance, logistics, and personnel management applications. Systems having high priority products associated with event-based urgency, such as systems critical to direct mission fulfillment by deployed or contingency military forces, are not routine. Box 5 of the National Security System Identification Checklist should be marked yes if and only if the system is critical to the direct fulfillment of military or *intelligence* missions and is not used exclusively for routine administrative and business applications.

4.2.6 Classified Systems

Executive orders and Acts of Congress have directed that some specific systems are to be protected at all times by procedures that have been established for information that is to be kept classified[*] in order to protect national defense or foreign policy interests. Box 6 of the National Security System Identification Checklist should be marked yes if and only if the system contains or processes classified information.

4.3 Dispute Resolution

In some cases, the owner of a system may disagree with a determination by an organization supported by the system regarding whether or not the system is critical to the direct fulfillment of military or *intelligence* missions. If the *agency* that owns and/or operates a system disputes identification of the system as a *national security system*, either the *agency* or the mission manager may submit the issue to both the CNSS and the appropriate office at the Office of Management and Budget (OMB). OMB will coordinate with other cognizant offices of the Executive Office of the President as required.

If there is a dispute regarding security classification of information processed by a system, the dispute must be submitted to the appropriate internal challenge program[4] for resolution. If the dispute cannot be resolved under the internal challenge program, or if a dispute involves more than one agency, the issue may be submitted to the Information Security Oversight Office (ISOO) for resolution. The ISOO may be contacted at Information Security Oversight Office, National Archives and Records Administration, 700 Pennsylvania Avenue, NW, Room 500, Washington, DC 20408.[5] Any remaining issues may be submitted to the National Security Council.

---

[*] See Glossary definition for *security classification*.

[4] Section 1.8(b) of E.O. 13292 [7] requires internal challenge programs for resolution of differences regarding classification of information.

[5] Electronic mail address is isoo@nara.gov.

This page intentionally left blank.

Appendix A: National Security System Identification Checklist

National Security System Identification Checklist		
System Identification:		
Answer each question in the box provided to the right of the question. Answer yes or no.		
(1) Does the system involve intelligence activities?		**(1)**
(2) Does the system involve cryptologic activities related to national security?		**(2)**
(3) Does the system involve military command and control of military forces?		**(3)**
(4) Does the system involve equipment that is an integral part of a weapon or weapons system?		**(4)**
(5) If the system is not used for routine administrative or business applications, is the system critical to the direct fulfillment of military or intelligence missions?		**(5)**
(6) Is the system protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy?		**(6)**
If the answer to any of the six questions is "Yes", then the system is a *national security system*.		
Is this system a national security system?		
Organization of Respondent:	Address of Organization: Telephone:	
Name of Respondent:	Signature of Respondent:	Date: (dd/mm/yy)

This page intentionally left blank.

Appendix B: References

[1] 10 USC Chapter 18 – *Military Support for Civilian Law Enforcement Activities,* 10/26/98.

[2] 40 USC Chapter 25 – *Information Technology Management*, Section 1401 – Definitions.

[3] 44 USC Chapter 35 - *Coordination of Federal Information Policy*, Subchapter I - Federal Information Policy, Sec. 3502 - Definitions, 01/02/01.

[4] 44 USC Chapter 35 – *Coordination of Federal Information Policy,* Subchapter III - Information Security, Sec. 3542 Definitions, 12/17/02.

[5] 47 USC Chapter 5 – *Wire or Radio Communications*, Subchapter I – General Provisions, Sec. 153 Definitions.

[6] 50 USC Chapter 15 – *National Security,* Section 401a – Definitions.

[7] *Classified National Security Information*, Executive Order 13292, Executive Office of the President, Washington, DC, March 25, 2003.

[8] Clinger-Cohen Act, Public Law 104-106, *National Defense Authorization Act For Fiscal Year 1996*, Division E – Information Technology Reform, Sec. 5002 – Definitions, 8/8/96.

[9] Clinger-Cohen Act, Public Law 104-106, *National Defense Authorization Act For Fiscal Year 1996*, Division E – Information Technology Reform, Sec. 5142 – National Security Systems Defined, 8/8/96.

[10] *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication 1-02, Rev. 8/14/02.

[11] *Federal Information Security Management Act of 2002*, Public Law 107-347, Subchapter III – Information Security, Sec. 303 – National Institute of Standards and Technology, 12/17/02.

[12] *Homeland Security Act of 2002*, Public Law 107-296, Title II – Information Analysis and Infrastructure Protection, Subtitle A – Directorate for Information Analysis and Infrastructure Protection: Access to Information, Section 202 – Access to Information, 11/25/02.

[13] *President's Foreign Intelligence Advisory Board*, Executive Order #12863, 9/13/93.

[14] *Telcom Glossary 2000*, American National Standards Institute, ANS T1.523-2001, 2001

[15] *United States Intelligence Activities*, Executive Order 12333, Executive Office of the President, Washington, DC, December 4, 1981.